

Security of two-way quantum cryptography against asymmetric Gaussian attacks

Stefano Pirandola,¹ Stefano Mancini,² Seth Lloyd,^{1,3} and Samuel L. Braunstein⁴

¹MIT - Research Laboratory of Electronics, Cambridge MA 02139, USA

²Dipartimento di Fisica & CNISM, Università di Camerino, I-62032 Camerino, Italy

³MIT - Department of Mechanical Engineering, Cambridge MA 02139, USA

⁴Computer Science, University of York, York YO10 5DD, United Kingdom

(Dated: September 18, 2008)

Recently, we have shown the advantages of two-way quantum communications in continuous variable quantum cryptography. Thanks to this new approach, two honest users can achieve a non-trivial security enhancement as long as the Gaussian interactions of an eavesdropper are independent and identical. In this work, we consider asymmetric strategies where the Gaussian interactions can be different and classically correlated. For several attacks of this kind, we prove that the enhancement of security still holds when the two-way protocols are used in direct reconciliation.

INTRODUCTION TO CONTINUOUS VARIABLE QUANTUM CRYPTOGRAPHY

In recent years, quantum information has discovered the non-trivial advantages offered by continuous variable systems, i.e., quantum systems described by a set of observables, like position and momentum, having a continuous spectrum of eigenvalues [1]. Accordingly, quantum key distribution has been extended to this new framework [2, 3, 4, 5] and cryptographic protocols based on coherent states have been proven to be very powerful for their experimental feasibility [6, 7]. In these quantum key distribution protocols, Alice prepares a coherent state $|\gamma\rangle$ whose amplitude $\gamma = (Q + iP)/2$ encodes two random variables Q and P following two independent Gaussian distributions (having zero mean and the same large variance). Then, Alice sends the state to Bob, who measures it in order to retrieve the encoded information. Such a measurement can be:

- (i) A measurement of Q or P , randomly chosen by Bob. Such a disjoint measurement is called homodyne detection and, therefore, we call “homodyne” (*Hom*) the corresponding protocol [4, 6].
- (ii) A joint measurement of Q and P . This measurement is called heterodyne detection and is equivalent to a balanced beam splitter followed by two homodyne detectors. We call “heterodyne” (*Het*) the corresponding protocol [5, 7].

In both protocols, Alice and Bob finally share pairs of correlated continuous variables. From these variables they can extract a secret binary key via slicing techniques of the phase space [8]. This classical stage is called *reconciliation* and can be *direct* if Bob estimates Alice’s original variables or *reverse* if Alice estimates Bob’s outcomes [9].

Even if these protocols belong to the so-called prepare and measure (PM) schemes, they can be equivalently formulated in terms of Einstein-Podolsky-Rosen (EPR) schemes, where Alice and Bob extract a secret key from the correlated outcomes of the measurements made upon

a shared EPR *source*. This source is realized by a two-mode squeezed vacuum state whose correlation matrix is equal to

$$\mathbf{V} = \begin{pmatrix} V\mathbf{I} & \sqrt{V^2 - 1}\mathbf{Z} \\ \sqrt{V^2 - 1}\mathbf{Z} & V\mathbf{I} \end{pmatrix}, \quad (1)$$

where $\mathbf{Z} \equiv \text{diag}(1, -1)$, \mathbf{I} the 2×2 identity matrix, and V is a variance characterizing the source [10]. One can easily show that heterodyning one mode of this EPR source is equivalent to the remote preparation of a coherent state $|\gamma\rangle$ whose amplitude γ is randomly modulated by a Gaussian of variance $V - 1$ (see Appendix). The EPR formulation of the *Hom* protocol is depicted in Fig. 1 where the attack of a potential eavesdropper, Eve, is also shown. According to the standard eavesdropping scenario, we consider an individual Gaussian attack which is based on the usage of an entangling cloner [6]. In this attack, each signal sent from Alice to Bob (mode B) is mixed with a *probe* (mode E), via a beam splitter of transmission T . This probe is part of an EPR source with variance W which is in Eve’s hands. At the end of the protocol, when Bob reveals the basis (Q or P) chosen for each run, Eve will consequently perform the appropriate homodyne measurements (Q or P) on her output modes E' and E'' . From such measurements, Eve will infer Alice’s variable (direct reconciliation) or Bob’s variable (reverse reconciliation). An entangling cloner attack can be therefore characterized by two parameters, transmission T and variance W , which can be arranged in the unique quantity

$$\Sigma \equiv W(1 - T)T^{-1}, \quad (2)$$

representing the variance of the Gaussian noise added by the channel. These quantities are evaluated by Alice and Bob by publishing part of their correlated continuous variables $Q_{B'}$ and Q_+ , or $P_{B'}$ and P_- (see Fig. 1). In this way, they perform an error analysis of the channel, which provides the correlation matrix \mathbf{V}' of their shared Gaussian state $\rho_{AB'}$ and, therefore, their mutual information $I_{AB} = I(Q_{B'}, Q_+)$ (see Appendix). Similarly, they can

evaluate I_{AE} and I_{BE} , and therefore the two key-rates $I_{AB} - I_{AE}$ (direct reconciliation) and $I_{AB} - I_{BE}$ (reverse reconciliation). The security thresholds achieved for high modulation ($V \rightarrow +\infty$) are equal to $\Sigma = 1$ for direct reconciliation, and to $\Sigma = T^{-1} > 1$ for reverse reconciliation. In particular, for direct reconciliation, the optimal attack is given by an entangling cloner with $W = 1$, i.e., a beam splitter (*lossy channel attack*). In such a case, the threshold simply corresponds to $T = 1/2$, i.e., 3 dB of losses [4]. Similar results [5] hold for the *Het* protocol.

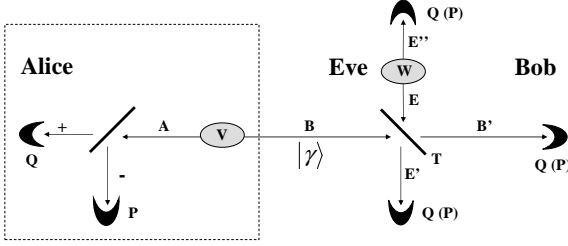


FIG. 1: Individual entangling cloner attack against the *Hom* protocol. (See text for explanation.) The dashed line displays a black-box, with an EPR source and a heterodyne detector inside, which Alice can use to prepare a randomly displaced coherent state $|\gamma\rangle$.

TWO-WAY PROTOCOLS

Even if the underlying physical principles are the same, different protocols are able to exploit them with different performances. In Ref. [11], we have shown that a security enhancement can be achieved by resorting to a multiple quantum communication (QC) between the trusted parties. In this approach, a bosonic mode is transmitted forward and backward between the two parties in order to store and distribute the secret information. Here we briefly review these protocols and then we study their security by assuming attacks which are asymmetric between the forward and backward paths. As depicted in Fig. 2, we may consider two different types of two-way protocols:

- (i) *Two-way homodyne (Hom^2) protocol.* The Hom^2 protocol extends the *Hom* protocol to two-way QC. In the Hom^2 protocol, Bob has an EPR source (with variance V), of which he keeps a mode r while he sends the other *reference* mode R to Alice. Then, Alice randomly displaces this mode in phase-space. This means that she applies a displacement operator [10] $D(\gamma)$ whose amplitude $\gamma = (Q + iP)/2$ follows a Gaussian distribution with $\langle Q^2 \rangle = \langle P^2 \rangle = V$ and $\langle QP \rangle = \langle Q \rangle = \langle P \rangle = 0$.

The final mode B is then sent back to Bob. This mode contains Alice's signal γ , since its quadratures are equal to $Q_B = Q_R + Q$ and $P_B = P_R + P$. In order to access this signal, Bob homodynes his modes r and B by choosing to measure their position or momentum at random. For instance, he can decide to measure positions Q_r and Q_B , so that he can construct an optimal estimator of Q_R (from Q_r) and, then, an estimator $Q^{(B)}$ of $Q = Q_B - Q_R$. Symmetrically, he can measure P_r and P_B to infer P . The basis chosen for each run of the protocol will be classically communicated to Alice at the end of protocol, when the two trusted parties will share pairs of correlated continuous variables $\{Q, Q^{(B)}\}$ and $\{P, P^{(B)}\}$.

- (ii) *Two-way heterodyne (Het^2) protocol.* As for the one-way protocols, Bob can perform a joint measurement of Q and P . This is achieved in the Het^2 protocol which extends the *Het* protocol to two-way QC. Here, Bob heterodynes his modes r and B , from whose results he infers the full signal (Q, P) of Alice. Notice that this protocol does not need any final basis revelation. Further, it can be fully implemented with coherent states. In fact, by heterodyning mode r , Bob equivalently prepares a coherent state $|\Gamma\rangle = D(\Gamma)|0\rangle$ which is sent to Alice. This state is a *reference* state which contains the reference random transformation Γ known to Bob. By applying her random displacement $D(\gamma)$, Alice transforms this state into another coherent state $|\Gamma + \gamma\rangle$ which is sent back to Bob via the mode B . By subsequent heterodyne detection, Bob is able to estimate the total amplitude $\Gamma + \gamma$ and, therefore, to infer γ from the knowledge of Γ .

As discussed in Ref. [11] the previous two-way protocols must be modified into safer hybrid formulations, $Hom^{1,2}$ and $Het^{1,2}$, where two-way QC is randomly switched with one-way QC. In the hybrid formulation of these protocols, the previous two-way QC is called the “ON configuration” and must be randomly switched with an “OFF configuration”. In the OFF configuration, Alice simply detects the reference mode R (via homodyne or heterodyne) and sends a new reference mode \tilde{R} back to Bob [11]. In both the ON and OFF configurations, Alice and Bob finally disclose part of the data in order to perform tomography of the quantum channel. Thanks to this information, Alice and Bob can reconstruct Eve's attack. In particular, they are able to understand if Eve is exploiting quantum and/or classical correlations between the forward and backward paths (two-mode attacks). If this is not the case (one-mode attacks), they use the ON instances to generate the secret key. Otherwise, they can use the OFF instances [11].

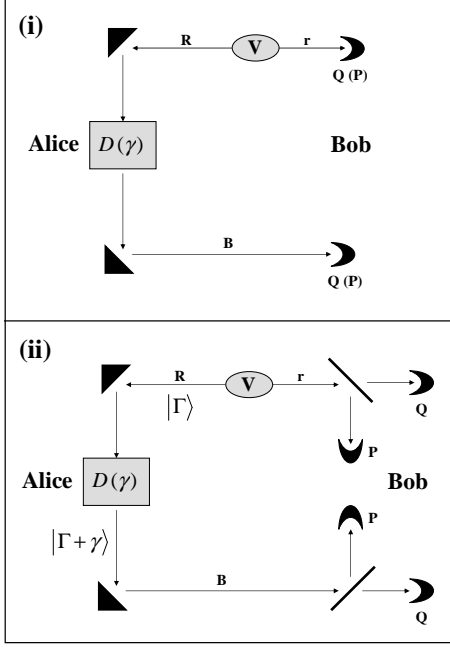


FIG. 2: Two-way quantum cryptography. Inset (i) shows the Hom^2 protocol, i.e., the ON configuration of the hybrid protocol $Hom^{1,2}$. Inset (ii) shows the Het^2 protocol, i.e., the ON configuration of the hybrid protocol $Het^{1,2}$.

SECURITY AGAINST ASYMMETRIC GAUSSIAN ATTACKS

Notice that in Ref. [11], the quantitative cryptoanalysis is restricted to one-mode Gaussian attacks, where independent and identical Gaussian interactions affect the forward and backward channels of the two-way quantum communication. Here, we study an extension of this analysis by considering attacks where the Gaussian interactions are independent but no longer identical. By independent interactions we mean interactions which are incoherent, i.e., void of quantum correlations. However, since these interactions are generally different, they can be classically correlated, i.e., specified by correlated parameters [12]. A general analysis of these “asymmetric Gaussian attacks” is very difficult. For this reason, we consider only specific classes which are constructed using entangling cloners and/or lossy channels. Further, our cryptoanalysis concerns direct reconciliation only. Under these assumptions we are able to prove that the ON configuration of the hybrid protocols (two-way QC) still provides a security enhancement.

Let us study the security of the hybrid protocol $Hom^{1,2}$ against (individual) asymmetric Gaussian attacks which are based on the combination of entangling cloners. Let us assume that Alice and Bob generate the secret key using the ON configuration of the protocol, i.e., the two-way QC. If we label the forward and backward chan-

nels by $i = 1, 2$ respectively, then we must combine two entangling cloners with free parameters T_1, W_1 and T_2, W_2 (i.e., added noises Σ_1 and Σ_2). By homodyning their outputs in the correct basis, Eve constructs an optimal estimator $Q^{(E)}$ [or $P^{(E)}$] of Alice’s variable. This enables her to eavesdrop the mutual information $I_{AE} = (1/2) \ln(V/V_{A|E})$, where the conditional variance $V_{A|E} \equiv V_{Q|Q^{(E)}} = V_{P|P^{(E)}}$ quantifies Eve’s remaining uncertainty on Alice’s variable. Similarly, Bob’s estimator $Q^{(B)}$ [or $P^{(B)}$] leaves him with a conditional variance $V_{A|B} \equiv V_{Q|Q^{(B)}} = V_{P|P^{(B)}}$. For $T_i \neq 0, 1$ and $V \rightarrow +\infty$, one derives

$$V_{A|B} = \frac{T_2(1 - T_1)W_1 + (1 - T_2)W_2}{T_2}, \quad (3)$$

$$V_{A|E} = \frac{T_2(1 - T_1)W_2^{-1} + (1 - T_2)W_1^{-1}}{(1 - T_1)(1 - T_2)}. \quad (4)$$

Let us consider the minimum of $V_{A|B}V_{A|E}$, so that Eve minimizes her perturbation of the channel ($V_{A|B}$) while maximizing the acquired information (inverse of $V_{A|E}$). Such a product takes the minimum value $V_{A|B}V_{A|E} = 4$ for

$$W_2 = 1 \quad \text{and} \quad T_2 = [1 + (1 - T_1)W_1]^{-1}. \quad (5)$$

The latter condition corresponds to considering an entangling cloner with free parameters (T_1, W_1) on the forward channel, followed by a beam splitter with a classically correlated transmission $T_2 = f(T_1, W_1)$ on the backward channel. In order to derive the security threshold we must impose the condition $I_{AB} = I_{AE}$ which is equivalent to $V_{A|B} = V_{A|E}$. By using Eqs. (3), (4) and (5), we get $W_1 = (1 - T_1)^{-1}$ and $T_2 = 1/2$. These parameters characterize the curve of the threshold attacks which have total noise equal to

$$\Sigma \equiv \Sigma_1 + \Sigma_2 = 1 + T_1^{-1}. \quad (6)$$

It follows that the security threshold of $Hom^{1,2}$ satisfies $\Sigma > 2$, to be compared with the security threshold $\Sigma = 1$ of the corresponding one-way protocol Hom^1 . In other words, when the communication channel is too noisy for one-way protocols, it can still be used by two-way protocols to generate a secret key.

In order to support further this “superadditivity”, we also study the case of asymmetric lossy-channel attacks where the two paths of QC are attacked by two beam splitters with different (correlated) transmissions T_1 and T_2 . Once the correct basis is disclosed by Bob, Eve homodynes their output ports E'_1 and E'_2 to infer the signal (in the individual version of the attack). Since two beam splitters are two entangling cloners with $W_1 = W_2 = 1$, from Eqs. (3) and (4) we get

$$V_{A|B} = \frac{1 - T_1T_2}{T_2}, \quad (7)$$

and

$$V_{A|E} = \frac{1 - T_1 T_2}{(1 - T_1)(1 - T_2)} . \quad (8)$$

Then, from $V_{A|B} = V_{A|E}$ we get the threshold curve for this kind of attack, i.e.,

$$T_2 = (1 - T_1)(1 - T_2) . \quad (9)$$

The total transmission $T \equiv T_1 T_2$ has a maximum equal to $3 - 2\sqrt{2}$ on this curve. Such a value corresponds to a threshold of about 7.65dB of losses, to be compared with the 3dB limit of the one-way protocol.

More strongly, we prove that this threshold remains the same even when we change the nature of the lossy-channel attack from individual to collective. In the collective attack, Eve keeps her output probes until the end of the protocol, when she exploits all the classical information exchanged by Alice and Bob to perform a final coherent measurement on all her probes. In such a case, the key rate is bounded by $I_{AB} - \chi_E$ where χ_E is the Holevo information of the ensemble $\rho_E = \int G(Q)\rho_E(Q)dQ$ (here $\rho_E(Q)$ is Eve's conditional state, while $G(Q)$ is a Gaussian with variance $\langle Q^2 \rangle = V$). For $T_i \neq 0, 1$ and $V \rightarrow +\infty$, one can prove (see Appendix) that

$$\chi_E = \frac{1}{2} \ln \left[\frac{V(1 - T_1)(1 - T_2)}{1 - T_1 T_2} \right] . \quad (10)$$

In the same limit, Alice and Bob's mutual information is given by

$$I_{AB} = \frac{1}{2} \ln \left(\frac{V}{V_{A|B}} \right) \rightarrow \frac{1}{2} \ln \left(\frac{T_2 V}{1 - T_1 T_2} \right) . \quad (11)$$

As a consequence, the threshold condition $I_{AB} = \chi_E$ gives the same curve of Eq. (9), so that the security threshold remains 7.65dB.

Let us now study the security of the hybrid protocol $Het^{1,2}$ against (collective) asymmetric lossy-channel attacks. Let us assume again that Alice and Bob use the ON configuration to generate the secret key. For $T_i \neq 0, 1$ and $V \rightarrow +\infty$, one derives $I_{AB} = \ln(T_2 V/2)$ while Eve's accessible information is bounded by

$$\chi_E = \ln \left[\frac{eV(1 - T_1)(1 - T_2)}{2(1 - T_1 T_2)} \right] . \quad (12)$$

Then, from the condition $I_{AB} = \chi_E$, one finds the curve

$$T_2(1 - T_1 T_2) = e(1 - T_1)(1 - T_2) . \quad (13)$$

On this curve the total transmission $T \equiv T_1 T_2$ has a maximum equal to $e(e + 4)^{-1}$, corresponding to about 3.93dB. Such a value must be compared with the threshold of 1.4dB found for the corresponding Het protocol [13]. Notice that if we allow Bob to perform coherent measurements (on all his states) in order to retrieve Alice's signal (Q, P) , then we can reach the same security

performances of the $Hom^{1,2}$ protocol. In such a case, in fact, Bob can asymptotically approach the accessible information

$$\chi_B = \ln \left[\frac{eT_2 V}{2(1 - T_1 T_2)} \right] , \quad (14)$$

for $V \rightarrow +\infty$ and $T_i \neq 0, 1$ (see Appendix). From the threshold condition $\chi_B - \chi_E = 0$, we then get the same curve of Eq. (9) and, therefore, the same security threshold of 7.65dB as $Hom^{1,2}$.

CONCLUSION

In conclusion, multi-way quantum cryptography represents a new environment to develop and extend quantum key distribution protocols. In this paper we have studied the security of two-way protocols against Gaussian attacks which are asymmetric between the two paths of the quantum communication. We have shown that, even in the presence of these asymmetric strategies, the superadditivity of the two-way quantum communication is preserved in direct reconciliation. In particular, this is true for an important class of asymmetric Gaussian attacks, i.e., the asymmetric lossy-channel attacks. These analyses represent further steps to assess the security of two-way schemes in the context of continuous variable quantum cryptography.

ACKNOWLEDGEMENTS

The research of S. Pirandola was supported by a Marie Curie Outgoing International Fellowship within the 6th European Community Framework Programme. S.L. was supported by the W.M. Keck center for extreme quantum information processing (xQIT).

APPENDIX

Estimators and remote state preparation

Consider the general scenario where Alice and Bob share two modes A and B , whose quadratures $\vec{\xi} \equiv (Q_A, P_A, Q_B, P_B)$ satisfy the canonical commutation relations $[\xi_l, \xi_m] = 2i\mathbf{J}_{lm}$, where

$$\mathbf{J} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} . \quad (15)$$

Suppose that modes A and B are described by a bipartite Gaussian state ρ_{AB} , with zero displacement $d \equiv \langle \vec{\xi} \rangle = 0$ and correlation matrix (CM) \mathbf{V} , with generic entries $\mathbf{V}_{lm} \equiv \langle \xi_l \xi_m + \xi_m \xi_l \rangle / 2$. The CM \mathbf{V} is a real and symmetric matrix that must satisfy the Heisenberg principle

$$\mathbf{V} + i\mathbf{J} \geq 0 , \quad (16)$$

taking the form $\langle Q_A^2 \rangle \langle P_A^2 \rangle \geq 1$ for the diagonal elements. All the quantum and/or classical correlations between the modes are described by the CM which we assume to be completely known to the parties.

Then, suppose that Alice homodynes mode A and Bob homodynes mode B , both of them projecting onto the same quadrature, e.g., Q . Thanks to the shared correlations, Alice is able to infer Bob's outcome Q_B from the outcome Q_A of her measurement [9]. In fact, from Q_A , Alice can construct the optimal estimator $Q_B^{(A)} \equiv \kappa Q_A$ of the variable Q_B , where $\kappa \equiv \langle Q_A Q_B \rangle \langle Q_A^2 \rangle^{-1}$ is directly computable from the CM. After her estimation, Bob's variable Q_B , with initial variance $V_{Q_B} \equiv \langle Q_B^2 \rangle$, will be reduced to the conditional variable $Q_{B|A} \equiv Q_B - Q_B^{(A)}$ with conditional variance

$$\begin{aligned} V_{Q_B|Q_A} &\equiv \langle Q_{B|A}^2 \rangle = \langle Q_B^2 \rangle - \frac{\langle Q_B^{(A)} Q_B \rangle^2}{\langle Q_B^{(A)2} \rangle} \\ &= \langle Q_B^2 \rangle - \frac{\langle Q_A Q_B \rangle^2}{\langle Q_A^2 \rangle}. \end{aligned} \quad (17)$$

Thanks to Alice's estimation, the Shannon entropy $H(Q_B) = (1/2) \ln V_{Q_B}$ of Bob's variable has been reduced to the conditional entropy $H(Q_B|Q_A) = (1/2) \ln V_{Q_B|Q_A}$. Therefore, the mutual information of Alice and Bob will be given by

$$I(Q_B, Q_A) = H(Q_B) - H(Q_B|Q_A) = \frac{1}{2} \ln \frac{V_{Q_B}}{V_{Q_B|Q_A}}. \quad (18)$$

Now, if we do not consider Bob's measurement, Alice's local measurement corresponds to a remote state preparation at Bob's site. In fact, her measurement simply corresponds to a Gaussian quantum operation that projects Bob's mode onto a Gaussian state, centered at the point $\{Q_B^{(A)}, 0\}$ of phase-space, and with uncertainties equal to $V_{Q_B|Q_A}$ of Eq. (17) and $V_{P_B|P_A} \geq V_{Q_B|Q_A}^{-1}$. More generally, Alice can remotely prepare a Gaussian state by making a joint measurement of her quadratures Q_A and P_A . For instance, she can perform a heterodyne detection by inserting her mode A into a balanced beam splitter and, then, detecting the quadratures Q_+ and P_- of the output modes ' \pm ' (see Fig. 1). From the outcomes (Q_+, P_-) , Alice can construct two optimal estimators $Q_B^{(+)} = \xi_+ Q_+$ and $P_B^{(-)} = \xi_- P_-$, so that Bob's variables Q_B and P_B are reduced to the conditional ones $Q_{B|+} \equiv Q_B - Q_B^{(+)}$ and $P_{B|-} \equiv P_B - P_B^{(-)}$, with conditional variances $V_{Q_B|Q_+}$ and $V_{P_B|P_-}$ [computable from the CMs of ρ_{+B} and ρ_{-B} according to Eq. (17)]. In other words, Alice remotely prepares a Gaussian state centered at $\{Q_B^{(+)}, P_B^{(-)}\}$ with uncertainties $V_{Q_B|Q_+}$ and $V_{P_B|P_-}$. In particular, if the shared Gaussian state ρ_{AB} is an EPR source with variance V [see Eq. (1)] then $V_{Q_B|Q_+} = V_{P_B|P_-} = 1$ and, therefore, Alice prepares a

coherent state $|\gamma\rangle$ with amplitude $\gamma = [Q_B^{(+)} + iP_B^{(-)}]/2$. Due to the probabilistic behavior of the measurement, the amplitude γ represents a complex random variable over many instances of the process. Such a variable follows a Gaussian distribution with zero mean and second moments given by $\langle Q_B^{(+2)} \rangle = \langle P_B^{(-2)} \rangle = V - 1$ and $\langle Q_B^{(+)} P_B^{(-)} \rangle = 0$. Therefore, the physical scheme where Alice and Bob share an EPR source with variance V and Alice heterodynes her mode is equivalent to a black-box where Alice prepares a coherent state whose amplitude is modulated by a Gaussian distribution with variance $V - 1$. In this sense, prepare and measure schemes using coherent states are equivalent to EPR schemes.

Computation of the relevant entropies

Consider the case of a collective and asymmetric lossy-channel attack against the protocol $Hom^{1,2}$ in the ON configuration. This means that Eve exploits two beam splitters of (correlated) transmissions T_1, T_2 and performs a final coherent measurement on all her probes. Eve's output modes E'_1, E'_2 are described by a state $\rho_E(Q)$ which is conditioned to Alice's encoding Q . On average, Eve gets an ensemble $\rho_E = \int G(Q) \rho_E(Q) dQ$, where $G(Q)$ is a Gaussian distribution with variance $\langle Q^2 \rangle = V$. The Holevo information of Eve is then equal to $\chi_E = S_E - S_{E|A}$, where S_E and $S_{E|A}$ are the Von Neumann entropies of ρ_E and $\rho_E(Q)$ (computable from the CMs \mathbf{V}_E and $\mathbf{V}_{E|A}$ of the corresponding Gaussian states). One can prove that $\mathbf{V}_E = \mathbf{V}_{12} \oplus \mathbf{I} \oplus \mathbf{I}$, where

$$\mathbf{V}_{12} = \begin{pmatrix} \mu_1 \mathbf{I} & \theta \mathbf{I} \\ \theta \mathbf{I} & \mu_2 \mathbf{I} + \Omega(V, V) \end{pmatrix}, \quad (19)$$

with

$$\mu_1 \equiv T_1 + (1 - T_1)V, \quad (20)$$

$$\mu_2 \equiv 1 + T_1(1 - T_2)(V - 1), \quad (21)$$

$$\theta \equiv \sqrt{T_1(1 - T_1)(1 - T_2)}(V - 1), \quad (22)$$

and

$$\Omega(V_Q, V_P) \equiv (1 - T_2) \begin{pmatrix} V_Q & 0 \\ 0 & V_P \end{pmatrix}. \quad (23)$$

The Von Neumann entropy S_E of the Gaussian state ρ_E can be computed from the symplectic eigenvalues [14] ν_k of the CM \mathbf{V}_E according to the formula

$$S_E = \sum_{k=1}^4 g(\nu_k), \quad (24)$$

where

$$g(x) \equiv \left(\frac{x+1}{2} \right) \ln \left(\frac{x+1}{2} \right) - \left(\frac{x-1}{2} \right) \ln \left(\frac{x-1}{2} \right). \quad (25)$$

Note that, for $x \rightarrow +\infty$, the latter function adopts the asymptotic expression [11, 13]

$$g(x) \rightarrow 1 + \ln(x/2) + O(x^{-1}). \quad (26)$$

Since $\mathbf{V}_E = \mathbf{V}_{12} \oplus \mathbf{I} \oplus \mathbf{I}$, we have that

$$\nu_1 = \nu_- , \nu_2 = \nu_+ , \nu_3 = \nu_4 = 1 , \quad (27)$$

where ν_{\pm} are the symplectic eigenvalues of \mathbf{V}_{12} . For non trivial attacks ($T_i \neq 0, 1$) and high modulation ($V \rightarrow +\infty$), the symplectic eigenvalues ν_{\pm} become proportional to V . In particular, one has

$$\nu_+ \nu_- = \sqrt{\det \mathbf{V}_{12}} \rightarrow (1 - T_1)(1 - T_2)V^2. \quad (28)$$

In the same limit, the entropy becomes

$$\begin{aligned} S_E &= g(\nu_-) + g(\nu_+) \rightarrow 2 + \ln \left[\frac{1}{4} \lim_{V \rightarrow +\infty} \sqrt{\det \mathbf{V}_{12}} \right] \\ &= 2 + \ln \left[\frac{V^2}{4} (1 - T_1)(1 - T_2) \right]. \end{aligned} \quad (29)$$

The conditional entropy $S_{E|A}$ can be computed from the symplectic eigenvalues of the matrix $\mathbf{V}_{E|A}$. It is easy to verify that $\mathbf{V}_{E|A}$ can be derived from \mathbf{V}_E by substituting $\Omega(0, V)$ for $\Omega(V, V)$ in Eq. (19). Then, repeating the previous steps, one finds

$$S_{E|A} \rightarrow 2 + \frac{1}{2} \ln \left[\frac{V^3}{16} (1 - T_1)(1 - T_2)(1 - T_1 T_2) \right], \quad (30)$$

so that χ_E is equal to Eq. (10).

Consider now a collective and asymmetric lossy-channel attack against the protocol $Het^{1,2}$ in the ON configuration. Eve's entropy S_E is the same as before, while the partial entropy $S_{E|A}$ is now conditioned to both of Alice's variables Q and P . This entropy can be derived from the conditional CM $\mathbf{V}_{E|A}$, which is computed from \mathbf{V}_E by substituting $\Omega(0, 0)$ for $\Omega(V, V)$ in Eq. (19). For $T_i \neq 0, 1$ and taking $V \rightarrow +\infty$, one finds

$$S_{E|A} \rightarrow 1 + \ln \left[\frac{V}{2} (1 - T_1 T_2) \right], \quad (31)$$

so that the Holevo information χ_E is equal to Eq. (12). Now, let us allow Bob to perform a coherent measurement on all his states, in order to retrieve the full signal $\gamma = (Q + iP)/2$ encoded by Alice. Bob's modes r and B' are described by a state $\rho_B(\gamma)$ which is conditioned to Alice's encoding γ . On average, Bob gets an ensemble $\rho_B = \int G(\gamma) \rho_B(\gamma) d^2 \gamma$, where $G(\gamma)$ is a Gaussian distribution with $\langle Q^2 \rangle = \langle P^2 \rangle = V$ and $\langle QP \rangle = 0$. The Bob's Holevo information is then equal to $\chi_B = S_B - S_{B|A}$, where the two Von Neumann entropies S_B and $S_{B|A}$ are computable from the CMs of ρ_B and $\rho_B(\gamma)$ exactly as before. One can verify that ρ_B has the CM

$$\mathbf{V}_B = \begin{pmatrix} V\mathbf{I} & \varphi\mathbf{Z} \\ \varphi\mathbf{Z} & [\varsigma + \Omega(V)]\mathbf{I} \end{pmatrix}, \quad (32)$$

where

$$\varphi \equiv \sqrt{T_1 T_2 (V^2 - 1)}, \quad (33)$$

$$\varsigma \equiv 1 + T_1 T_2 (V - 1), \quad (34)$$

and

$$\Omega(V) = T_2 V. \quad (35)$$

For $T_i \neq 0, 1$ and $V \rightarrow +\infty$, the symplectic eigenvalues of \mathbf{V}_B become proportional to V and the entropy becomes

$$S_B \rightarrow 2 + \ln \left[\frac{1}{4} \lim_{V \rightarrow +\infty} \sqrt{\det \mathbf{V}_B} \right] = 2 + \ln \left(\frac{T_2 V^2}{4} \right). \quad (36)$$

Then, the CM $\mathbf{V}_{B|A}$ of $\rho_B(\gamma)$ can be computed by substituting $\Omega(0)$ for $\Omega(V)$ in Eq. (32). In the usual limit, we have $\nu_- = 1$ and $\nu_+ \rightarrow V(1 - T_1 T_2)$, so that

$$S_{B|A} = g(\nu_+) \rightarrow 1 + \ln \left[\frac{V}{2} (1 - T_1 T_2) \right]. \quad (37)$$

From Eqs. (36) and (37), one easily gets Eq. (14) for Bob's Holevo information.

-
- [1] S. L. Braunstein, and A. K. Pati, *Quantum Information Theory with Continuous Variables*, Kluwer Academic, Dordrecht, 2003; S. L. Braunstein, and P. van Loock, "Quantum information with continuous variables," Rev. Mod. Phys. **77**, 513 (2005).
 - [2] T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**, 010303(R) (2000); T. C. Ralph, "Security of continuous-variable quantum cryptography," Phys. Rev. A **62**, 062306 (2000); M. D. Reid, "Quantum cryptography with a predetermined key using continuous-variable Einstein-Podolsky-Rosen correlations," Phys. Rev. A **62**, 062308 (2000).
 - [3] D. Gottesman, and J. Preskill, "Secure quantum key distribution using squeezed states," Phys. Rev. A **63**, 022309 (2001); S. Iblisdir, G. Van Assche, and N. J. Cerf, "Security of quantum key distribution with coherent states and homodyne detection," Phys. Rev. Lett. **93**, 170502 (2004).
 - [4] F. Grosshans, and Ph. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).
 - [5] C. Weedbrook *et al.*, "Quantum cryptography without switching," Phys. Rev. Lett. **93**, 170504 (2004).
 - [6] F. Grosshans *et al.*, "Quantum key distribution using Gaussian-modulated coherent states," Nature **421**, 238 (2003).
 - [7] A. M. Lance *et al.*, "No-switching quantum key distribution using broadband modulated coherent light," Phys. Rev. Lett. **95**, 180503 (2005).
 - [8] G. Van Assche *et al.*, "Reconciliation of a quantum-distributed Gaussian key," IEEE Trans. Inform. Theory **50**, 394 (2004).
 - [9] F. Grosshans *et al.*, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," Quant. Info. and Computation **3**, 535 (2003).

- [10] D. F. Walls, and G. J. Milburn, *Quantum Optics*, Springer, 1994.
- [11] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, "Quantum cryptography using two-way quantum communication," Nature Physics advance online publication, 11 July 2008 (arXiv:quant-ph/0611167v2).
- [12] Notice that, in general, the second interaction can be conditioned to both the parameters of the first interaction and the outcomes of a (possible) measurement which detects the corresponding output modes of the eavesdropper. However, in the limit of large modulation, it is reasonable to consider *universal* interactions which, therefore, are not conditioned to any outcome. As a consequence, the classical correlations can be reduced to correlations between the parameters of the two interactions.
- [13] F. Grosshans, "Collective attacks and unconditional security in continuous variable quantum key distribution," Phys. Rev. Lett. **94**, 020504 (2005); M. Navascués, and A. Acín, "Security bounds for continuous variables quantum key distribution," Phys. Rev. Lett. **94**, 020505 (2005).
- [14] A. S. Holevo *et al.*, "Capacity of quantum Gaussian channels," Phys. Rev. A **59**, 1820 (1999).